ON THE DISTRIBUTION OF THE NUMBER OF POINTS ON A FAMILY OF CURVES OVER FINITE FIELDS

KIT-HO MAK AND ALEXANDRU ZAHARESCU

Abstract. Let p be a large prime, $\ell \geq 2$ be a positive integer, $m \geq 2$ be an integer relatively prime to ℓ and $P(x) \in \mathbb{F}_p[x]$ be a polynomial which is not a complete ℓ'-th power for any ℓ' for which $GCD(\ell', \ell) = 1$. Let $\mathcal{C}$ be the curve defined by the equation $y^\ell = P(x)$, and take the points on $\mathcal{C}$ to lie in the rectangle $[0, p-1]^2$. In this paper, we study the distribution of the number of points on $\mathcal{C}$ inside a small rectangle among residue classes modulo m when we move the rectangle around in $[0, p-1]^2$.

1. Introduction

Since Weil's proof of the Riemann hypothesis for algebraic curves over finite fields [28], there have been numerous studies on the number of rational points of an algebraic curve over a finite field in a specified set of number theoretic interest. Examples include studies of bounds on the number of rational points in a smaller region inside $[0, p-1]^2$ (see for example Myerson [17], Fujiwara [11], and [16]), bounds on the number of points in sets with prescribed congruence conditions on the coordinates (known as Lehmer problems, see for example Zhang [31, 32], Cobeli and one of the authors [7] and Bourgain, Cochrane, Paulhus and Pinner [2]), bounds on the number of visible points (see Shparlinski [23], Shparlinski and Voloch [24], Shparlinski and Winterhof [25], Chan and Shparlinski [5]) and the fluctuations of the number of points among some families of curves (see Kurlberg and Rudnick [13], Xiong [29] and Bucur, David, Feigon, Lalín [3, 4]). Bounds for the number of rational points on curves in a small rectangle is crucial in the study of local spacings between fractional parts of $n^2\alpha$, see Rudnick, Sarnak and one of the authors [20, 30]. Such questions have applications in mathematical physics, see the important works by Berry and Tabor [1], Rudnick and Sarnak [19] and Sarnak [21].

All the above works study analytic aspects of the number of points of families of curves over finite fields, such as bounds on the number of points and the fluctuation of the number of points along a family. In this paper we study an arithmetic property of the number of points on curves of the form

$$y^\ell = P(x) \tag{1.1}$$

over $\mathbb{F}_p$, when the curve is absolutely irreducible. To make it precise, we take the rational points on the curve $\mathcal{C}$ as a subset in $[0, p-1]^2$, and let $\Omega \subseteq [0, p-1]^2$ be a rectangular "window". Instead of asking how many points are captured by Ω, we ask the following question: if we move the window around the domain, what is the probability that the number of captured points is even (or odd)? This kind

2010 *Mathematics Subject Classification.* Primary 11G20, 11T55.

Key words and phrases. rational points, algebraic curves, uniform distribution, power residues.

The second author is supported by NSF grant number DMS - 0901621.

of problem dates back to Gauss when he proved the well-known Gauss lemma for quadratic residues, i.e. if $GCD(a,p)=1$, then if r is the number of elements in the set $\{a, 2a, \dots, (\frac{p-1}{2})a\}$ that have least positive residue greater than $p/2$, then the Legendre symbol satisfies $\frac{a}{p} = (-1)^r$. Formulating in our language, this is to consider the number of points on the line $y = ax$ inside the rectangle $[1, (p-1)/2] \times (p/2, p-1]$, and then look at its residue class modulo 2. We also note that the uniformity modulo m of the values of some multiplicative functions, such as the Ramanujan tau function, was investigated by Serre [22]. For more results on the uniform distribution of the values of multiplicative functions modulo m, the reader is referred to the monograph of Narkiewicz [18]. Recently, Lamzouri and one of the authors [15] have studied the distribution of real character sums modulo m.

In the present paper, given a positive integer m, we ask about the distribution of the number of points captured by the window Ω among each congruence class of m when we move it around the domain. Since it is believed that the set of rational points on a curve exhibits a strong random behaviour, one may expect that the above mentioned probability is $1/m$. We prove that this is indeed the case when Ω has full length in the y-coordinate in Theorem 1. Next, we consider the joint distribution of the number of points on several different curves of the same form as (1.1). We will see that under some natural conditions, the distributions on these different curves are independent. After that, we show that restricting the y-coordinate of the rectangle will retain the uniform distribution among residue classes modulo m. Finally, we will give an application on the distribution of ℓ-th power residues and nonresidues in the last section.

The idea here is to relate our problems of studying the distribution of number of points modulo m to that of random walks on the additive group $\mathbb{Z}/m\mathbb{Z}$. The idea is to use results on random walks showing that the distribution modulo m in the random walk situation is uniform, and then show that the difference from our problem to that of the random walks can be handled, so that we get uniform distribution modulo m in our context as well. For information on random walks on finite groups, the reader is referred to [12, 26]. One important feature of our result is that uniform distribution occurs already when we consider the number of points in very short intervals.

2. Statement of Main Results

We first fix some notations. Let p be a large prime and let $\ell \geq 2$ be an integer. For a polynomial $P(x) \in \mathbb{F}_p[x]$, let $\mathcal{C}$ be the curve over $\mathbb{F}_p$ defined by the equation $y^\ell = P(x)$. Let I be a fixed positive integer (which will serve as the length of our rectangles). Define $N_{\mathcal{C}}(x_0, I)$ to be the number of points on $\mathcal{C}$ inside the rectangle $R_{x_0} = (x_0, x_0+I] \times [0, p-1]$, i.e.

$$N_{\mathcal{C}}(x_0, I) = \#\{(x,y) \in \mathcal{C}(\mathbb{F}_p) : x_0 < x \leq x_0 + I\}.$$

Let $\mathcal{I} \subseteq [0, p-1]$ be an interval, and denote $|\mathcal{I}| = \#(\mathcal{I} \cap \mathbb{Z})$. For any m with $GCD(m, \ell) = 1$, we define $\Phi_p(P, m, a)$ to be the proportion of values $x_0 \in \mathcal{I}$ such that $N_{\mathcal{C}}(x_0, I) \equiv a \mod m$, i.e.

$$\Phi_{\mathcal{C}}(m, a) = \frac{1}{|\mathcal{I}|} \#\{0 \leq x_0 \leq p-1 : N_{\mathcal{C}}(x_0, I) \equiv a \mod m\}.$$

Our first result is that when one moves the rectangles R_{x_0} along the x-direction, the $N_{\mathcal{C}}(x_0, I)$ becomes uniformly distributed modulo m. Note that the distribution

and the main term of the discrepancy does not depend on the lengths of the intervals I and $\mathcal{I}$, nor the particular position of $\mathcal{I}$ as long as the conditions in the theorem are satisfied.

Theorem 1. *Let p be a large prime and $P(x) \in \mathbb{F}_p[x]$ be a nonconstant polynomial of degree d which is not a complete ℓ'-th power for any ℓ' with $GCD(\ell', \ell) = 1$. Let $L = L(p) < \frac{\log p}{2 \log 4d}$ be an integral function of p such that $L(p) \to \infty$ as $p \to \infty$. Suppose $\mathcal{I}$ is an interval such that $\mathcal{I} \gg p^{\frac{1}{2}+\varepsilon}$ for some $\varepsilon > 0$, and I is an integer with $p - L > I > L$. Then for any positive integer m with $GCD(m, \ell) = 1$ we have*

$$\sum_{a=0}^{m-1} \left(\Phi_{\mathcal{C}}(m, a) - \frac{1}{m} \right)^2 \leq \frac{7m^3\ell^2}{L(p)} + O\left(\frac{m^3\ell^3 L(p)\sqrt{p}\log p}{|\mathcal{I}|} \right).$$

Corollary 1. *Assumptions and notations are as in Theorem 1. If $m = o(L(p)^{1/5})$, then*

$$\Phi_{\mathcal{C}}(m, a) = \frac{1}{m} + O\left(\sqrt{\frac{m^3\ell^2}{L(p)}} \right),$$

uniformly for all $0 \leq a \leq m - 1$.

Remark 2.1. Our assumption that $GCD(m, \ell) = 1$ is necessary in order to obtain uniform distribution. For example, if we consider the elliptic curve E defined by $y^2 = x^3 - n^2x$, then for each $x \neq 0, n, -n$, either there are two y so that $(x, y) \in E(\mathbb{F}_p)$, or there are none. Thus $N_E(x_0, I)$ is almost always even, and so one cannot have uniform distribution modulo 2. We remark that the distribution modulo 2 in this example depends on the location of the roots of the polynomial $P(x) = x^3 - n^2x$.

Although one cannot expect uniform distribution for a particular p when m and ℓ are not relatively prime, it may still be possible to have uniform distribution when we take an average over p. For example, let E_p be the elliptic curve $y^2 = x^3 + x$ over $\mathbb{F}_p$, and let $m = 2$. The distribution of $N_E(x_0, I)$ for a particular prime p might not be uniform, but instead depends on the locations of the roots of $x^2 + 1 \mod p$. Now we take N to be a large integer, and take an average over all primes $p \equiv 1 \pmod 4$, $p \leq N$ (here for each p we normalize the points in E_p by $(x, y) \mapsto (\frac{x}{p}, \frac{y}{p})$, so that we have a fixed domain for all p). By a well-known result of Duke, Friedlander and Iwaniec [9], the fractional parts $\frac{\nu}{p}$ of the roots of $x^2 + 1 \mod p$ are uniformly distributed as p varies. Therefore, the average values over $p \leq N$ of the number of points inside a rectangle $(x_0 + I) \times [0, 1)$ will be uniformly distributed modulo 2 when x_0 varies.

After studying the distribution of the number of points on the curve $\mathcal{C}$, we continue to consider the joint distribution of the number of points on curves of the form

$$\mathcal{C}_l : y^\ell = P_l(x)$$

for $1 \leq l \leq k$, where k is a positive integer, and all $P_l(x) \in \mathbf{F}_p[x]$ are polynomials that are not complete ℓ-th powers. Define

$$N_l(x_0, I) = N_{\mathcal{C}_l}(x_0, I) = \#\{(x, y) \in \mathcal{C}_l(\mathbb{F}_p : x_0 < x \leq x_0 + I\},$$

and for any vector $\mathbf{a} = (a_1, \ldots, a_k) \in \mathbb{Z}^k$,

$$\Phi(m, \mathbf{a}) = \frac{1}{|\mathcal{I}|} \#\{0 \leq x_l \leq p - 1 : N_l(x_l, I) \equiv a_l \mod m \ \forall 1 \leq l \leq k\}.$$

Our first observation is that various N_l's might not be independent of each other.

Remark 2.2. For example, let $\ell = 3$, $P_1(x) = x$ and $P_2(x) = x^2$, i.e.

$$\mathcal{C}_1 : y^3 = x,$$
$$\mathcal{C}_2 : y^3 = x^2.$$

Then we claim that $N_1(x_0, I) = N_2(x_0, I)$ for any x_0 and I. Indeed, fix an x. If $x = 0$, then both curves have a unique y. If $x \neq 0$ and $\mathcal{C}_1$ has a point (x, y), then (x, y^2) is a point on $\mathcal{C}_2$. Conversely, if $x \neq 0$ and (x, y) is a point on $\mathcal{C}_2$, then $(x, y^2/x)$ is a point on $\mathcal{C}_1$. Therefore, $N_1 = N_2$ as the number of points above any x is the same for both curves. As an immediate consequence, for any $\mathbf{a} = (a_1, a_2)$, we have

$$\Phi(m, \mathbf{a}) = \begin{cases} \frac{1}{m} & , a_1 = a_2, \\ 0 & , a_1 \neq a_2. \end{cases}$$

In view of the above remark, it is natural to introduce the following conditions. Let $P_1(x), \dots, P_k(x) \in \mathbf{F}_p[x]$ be polynomials. We say that the set $\{P_1(x), \dots, P_k(x)\}$ is *multiplicatively dependent* if there exists integers (which may be positive or negative) $e_1, \dots, e_l$ such that the combination

$$Q(x) = P_1(x)^{e_1} \dots P_k(x)^{e_k}$$

is identically 1. The set of polynomials is *multiplicatively independent* if it is not multiplicatively dependent.

If the polynomials are multiplicatively independent, we have the following result.

Theorem 2. *Let $k \geq 2$ be an integer. Let p be a large prime and $P_1(x), \dots, P_k(x) \in \mathbb{F}_p[x]$ be nonconstant polynomials of degree $d_1, \dots, d_k$ respectively, which are not complete ℓ'-th powers for any ℓ' with $GCD(\ell', \ell) = 1$. Let $d = \max\{d_1, \dots, d_k\}$. Suppose that the set of polynomials $\{P_1(x), \dots, P_k(x)\}$ is multiplicatively independent. Let $L = L(p) < \frac{\log p}{2 \log 4d}$ be an integral function of p such that $L(p) \to \infty$ as $p \to \infty$. Suppose $\mathcal{I}$ is an interval such that $\mathcal{I} \gg p^{\frac{1}{2}+\varepsilon}$ for some $\varepsilon > 0$, and I is an integer with $p - L > I > L$, then for any positive integer m with $GCD(m, \ell) = 1$, we have*

$$\sum_{\boldsymbol{a} \in (\mathbb{Z}/m\mathbb{Z})^k} \left(\Phi(m, \boldsymbol{a}) - \frac{1}{m^k} \right)^2 \leq \frac{7m^{k+2}\ell^2}{L} + O\left(\frac{dkL\ell^3 m^{k+2} \sqrt{p} \log p}{|\mathcal{I}|} \right)$$

An immediate corollary of the above theorem is that the $N_l(x_0, I)$ are independent. More precisely, we have the following.

Corollary 2. *Assumptions and notations are as in Theorem 2. If $m = o(L(p)^{1/(3k+2)})$, then*

$$\Phi(m, \boldsymbol{a}) = \frac{1}{m^k} + O\left(\frac{m^{k/2+1}\ell}{\sqrt{L(p)}} \right),$$

uniformly for all $\boldsymbol{a} \in (\mathbb{Z}/m\mathbb{Z})^k$.

So far we did not restrict the y-coordinates of the curves $\mathcal{C}$. Our next objective is to see if a restriction of y-coordinates will affect the distribution of the number of points into various congruence classes. For the sake of simplicity, we only consider the case when each x-coordinate has at most one corresponding y-value in the restricted domain such that $(x, y) \in \mathcal{C}$.

To be more precise, we let $\mathcal{I}, \mathcal{J} \subseteq [0, p-1]$ be two intervals such that the following condition holds:

$$(*) \qquad \forall x \in \mathcal{I}, \exists \text{ at most one } y \in \mathcal{J} \text{ such that } (x, y) \in \mathcal{C}.$$

Denote $\Omega = \mathcal{I} \times \mathcal{J}$, and define

$$N_{\mathcal{C},\Omega}(x_0, I) = \#\{(x, y) \in \mathcal{C}(\mathbb{F}_p) \cap \Omega : x_0 < x \leq x_0 + I\},$$

and

$$\Phi_{\mathcal{C},\Omega}(m, a) = \frac{1}{p}\#\{0 \leq x_0 \leq p-1 : N_{\mathcal{C},\Omega}(x_0, I) \equiv a \mod m\}.$$

Bringing into play some ideas from algebraic geometry, we prove that the numbers $N_{\mathcal{C},\Omega}(x_0, I)$ are uniformly distributed among the residue classes of m. Note that due to condition $(*)$, we do not need to assume that $GCD(m, \ell) = 1$ in this case.

Theorem 3. *Let p be a large prime and $P(x) \in \mathbb{F}_p[x]$ be a nonconstant polynomial of degree d which is not a complete ℓ'-th power for any ℓ' with $GCD(\ell', \ell) = 1$. Let $L = L(p) = o(\log p/\log\log p)$ be an integral function of p such that $L(p) \to \infty$ as $p \to \infty$, and let I is an integer with $p - L > I > L$ is an integer and let $\Omega = \mathcal{I} \times \mathcal{J}$ be a rectangle such that condition $(*)$ is satisfied, $|\mathcal{J}| = \alpha p$ for some $0 < \alpha \leq 1$, and $|\mathcal{I}| \gg p^{1/2+\delta}$ for some $\delta > 0$. Then for any positive integer m, we have*

$$\sum_{a=0}^{m-1} \left(\Phi_{\mathcal{C},\Omega}(m, a) - \frac{1}{m}\right)^2 \leq \frac{4m^4}{L(p)} + O(m^4/p^{\frac{1}{2}-\varepsilon}).$$

for all $\varepsilon > 0$.

Corollary 3. *Assumptions and notations are as in Theorem 3. If $m = o((L(p))^{1/6})$, then*

$$\Phi_{\mathcal{C},\Omega}(m, a) = \frac{1}{m} + O\left(\frac{m^2}{\sqrt{L(p)}}\right),$$

uniformly for all $0 \leq a \leq m-1$.

Finally, we will apply our results above to study the distributions of power residues and nonresidues. In particular, we obtain the following result, which says that for any fixed power residue class, we can find a representative in almost all short intervals in $[0, p-1]$.

Corollary 4. *Let $\ell \geq 2$ be an integer, and let $L(p)$ be an integer function of p that tends to infinity as p tends to infinity. For any ℓ-th root of unity μ and for all $x_0 \in [0, p-1]$ except possibly $O(p/L(p)^{1/7})$ of them, there is an x inside the interval $[x_0, x_0 + L(p))$ with $(\frac{x}{p})_\ell = \mu$, where $(\frac{\cdot}{p})_\ell$ denotes the ℓ-th power residue symbol.*

For more results on the distribution of quadratic residues and nonresidues in short intervals, or the distribution of more general multiplicative functions in short intervals, the reader is referred to the works of Davenport and Erdos [8], Chaterjee and Soundararajan [6] and Lamzouri [14].

3. Preliminaries

In this section we collect together some preliminary results which will be used later. The first few lemmas show that certain combinations of polynomials which are not a complete ℓ'-th powers cannot become a complete ℓ-th power.

Lemma 3.1. *Let $r \geq 2$, $x_1, \ldots, x_r \in \mathbb{F}_p$ be r distinct elements. Suppose $\mathcal{M}$ is a nonempty finite subset of the algebraic closure $\overline{\mathbb{F}}_p$ with $4|\mathcal{M}| < p^{\frac{1}{r}}$. Then there exists a $j \in \{1, \ldots, r\}$ such that the translate $\mathcal{M} + x_j$ is not contained in $\cup_{i \neq j}(\mathcal{M} + x_i)$.*

Proof. Suppose $(x_1, \ldots, x_r, \mathcal{M})$ provides a counterexample to the statement of the lemma. Then it is clear that for any nonzero $t \in \mathbb{F}_p$, the tuple $(tx_1, \ldots, tx_r, t\mathcal{M})$ is another counterexample.

We now use Minkowski's theorem on lattice points in a convex symmetric body to find a nonzero integer t such that

$$\begin{cases} |t| & \leq p-1 \\ \left\| \frac{tx_1}{p} \right\| & \leq (p-1)^{-\frac{1}{r}} \\ & \vdots \\ \left\| \frac{tx_r}{p} \right\| & \leq (p-1)^{-\frac{1}{r}}. \end{cases}$$

Thus there are integers y_j such that

$$\begin{cases} |y_j| & \leq p(p-1)^{-\frac{1}{r}} \\ y_j & \equiv tx_j \pmod{p} \end{cases} \tag{3.1}$$

for any $j \in \{1, \ldots, r\}$, and $(y_1, \ldots, y_r, t\mathcal{M})$ provides a counterexample. Now let j_0 be such that $|y_{j_0}| = \max_{1 \leq j \leq r} |y_j|$. Choose $\alpha \in t\mathcal{M}$ and consider the set $\tilde{\mathcal{M}} = t\mathcal{M} \cap (\alpha + \mathbb{F}_p)$. Then $(y_1, \ldots, y_r, \tilde{\mathcal{M}})$ will also be a counterexample.

Note that $\alpha + \mathbb{F}_p$ can be written as a union of at most $|\mathcal{M}|$ intervals (i.e. subsets of $\mathbb{F}_p$ consisting of consecutive integers or its translate in $\overline{\mathbb{F}}_p$) whose endpoints are in $\tilde{\mathcal{M}}$. Let $\{\alpha + a, \alpha + a + 1, \ldots, \alpha + b\}$ be the longest of these intervals. Then

$$|b - a| \geq \frac{p}{|\tilde{\mathcal{M}}|} \geq \frac{p}{|\mathcal{M}|}.$$

By this, (3.1) and the hypothesis $4|\mathcal{M}| < p^{\frac{1}{r}}$, we have

$$|b - a| > 4p^{1-\frac{1}{r}} > 2|y_{j_0}|.$$

Now if $y_{j_0} > 0$, then $\alpha + a + y_{j_0}$ belongs to $\tilde{\mathcal{M}} + y_{j_0}$ but does not belong to $\cup_{i \neq j_0}(\tilde{\mathcal{M}} + y_i)$, while if $y_{j_0} > 0$, then $\alpha + b + y_{j_0}$ belongs to $\tilde{\mathcal{M}} + y_{j_0}$ but does not belong to $\cup_{i \neq j_0}(\tilde{\mathcal{M}} + y_i)$. This contradicts the fact that $(y_1, \ldots, y_r, \tilde{\mathcal{M}})$ is a counterexample, and thus completes our proof. □

Now we are ready to prove the promised result about combinations of polynomials.

Lemma 3.2. *Let $\ell \geq 2$ be an integer. Let $P(x) \in \mathbb{F}_p[x]$ be a polynomial which is not a complete ℓ'-th power for any ℓ' with $GCD(\ell', \ell) = 1$. Let $b_1, \ldots, b_r$ be r distinct elements in $\mathbb{F}_p$ with $r < (\log p)/\log(4 \deg P)$. Then for any $a \in \mathbb{F}_p$ and $\mathbf{e} = (e_1, \ldots, e_r)$ with $0 \leq e_j \leq \ell - 1, \mathbf{e} \neq 0$, the polynomial*

$$Q(x) = \prod_{j=1}^{r} P(ax + b_j)^{e_j}$$

is not a complete ℓ-th power.

Proof. The lemma is clearly true for all ℓ when $r = 1$. Suppose the lemma is not true, then there is a least $r > 1$ (but satisfying our assumption $r < (\log p)/\log(4 \deg P)$) such that a counterexample exists. Let $\tilde{\ell}$ be the least ℓ such that a counterexample occurs for the above r, then we have

$$Q(x) = \tilde{P}(x)^{\tilde{\ell}} = \prod_{j=1}^{r} P(ax + b_j)^{\tilde{e}_j}, \tag{3.2}$$

where $1 \leq \tilde{e_j} < \tilde{\ell}$ (if $e_j = 0$ for some j we would have a smaller counterexample) and $\tilde{P}(x) \in \mathbb{F}_p[x]$.

Let $\alpha_1, \ldots, \alpha_s$ be all the *distinct* zeros of $P(x)$ in $\overline{\mathbb{F}}_p$. Without loss of generality we may assume that the multiplicities m_j of each α_j satisfy $1 \leq m_j < \ell$. Clearly $1 \leq s \leq \deg P$. Let $\mathcal{M} = \{a^{-1}\alpha_1, \ldots, a^{-1}\alpha_s\}$ and $x_j = -a^{-1}b_j$ for all $1 \leq j \leq r$. Note that $\mathcal{M} + x_j$ is the set of zeros of $P(ax + b_j)$. Since $4\,|\mathcal{M}| = 4s \leq 4 \deg P < p^{\frac{1}{r}} < p^{\frac{1}{r'}}$, we can apply Lemma 3.1 to obtain a j_0 such that at least one of the roots of $P(ax + b_{j_0})$ is distinct from the roots of all other $P(ax + b_i)$ for $i \neq j_0$. By permuting the x_j and α_j we may assume that the above occurs for $j_0 = r$, and the distinguished root is α_s, which has multiplicity m_s.

If m_s is relatively prime to $\tilde{\ell}$, then $\tilde{e}_r m_s$ cannot be a multiple of $\tilde{\ell}$. This means the combination $Q(x)$ cannot be a complete $\tilde{\ell}$-th power, which contradicts (3.2). On the other hand, if $GCD(m_s, \tilde{\ell}) = \frac{\tilde{\ell}}{d} > 1$, then (3.2) implies that $\tilde{e}_r$ must be a multiple of d. Since $d < \tilde{\ell}$, we see that

$$\frac{Q(x)}{P(ax + b_r)^{\tilde{e}_r}} = \left(\frac{\tilde{P}(x)^{\frac{\tilde{\ell}}{d}}}{P(ax + b_r)^{\frac{\tilde{e}_r}{d}}} \right)^d = \prod_{j=1}^{r-1} P(ax + b_j)^{\tilde{e}_j} \tag{3.3}$$

is a complete d-th power. Thus either there exists some $\tilde{e}_j$ which is not a multiple of d, so (3.3) is a counterexample with smaller r, or each $\tilde{e}_j$ is a multiple of d, then

$$Q(x)^{\frac{1}{d}} = \tilde{P}(x)^{\frac{\tilde{\ell}}{d}} = \prod_{j=1}^{r} P(ax + b_j)^{\frac{\tilde{e}_j}{d}}$$

is a counterexample with the same r but a power smaller than $\tilde{\ell}$. In both cases we obtain a contradiction. □

For any positive integer m, denote $e_m(z) = e^{2\pi i z/m}$. Denote by μ_ℓ the set of ℓ-th roots of unity. For any vector $v \in \mu_\ell^k$, define

$$F(v) = 1 + v + \ldots + v^{\ell-1} = \begin{cases} \ell & , \ v = 1, \\ 0 & , \ \text{otherwise.} \end{cases} \tag{3.4}$$

We introduce the following probability model for the values of $F(v)$ based on random walks. If an ℓ-th root of unity v is drawn at random, and the probability that each root being drawn is $1/\ell$, then $F(v) = \ell$ with probability $1/\ell$ and $F(v) = 0$ with probability $(\ell - 1)/\ell$. Inspired by this fact, we let $\{X_j\}, \{Y_j\}$ be two sequences of independent random variables so that

$$P(X_j = \ell) = 1/\ell \qquad \text{and} \qquad P(X_j = 0) = \frac{\ell - 1}{\ell},$$

and the same for Y_j. We consider the stochastic process $\{Z_x \mod m\}_{x\geq 1}$, where

$$Z_x = \sum_{j=1}^{x} X_j - \sum_{j=1}^{x} Y_j.$$

This can be viewed as a random walk on the additive group $\mathbb{Z}/m\mathbb{Z}$, with each step being the random variable $X_j - Y_j$. We are interested in the random variable

$$\Phi(L; m, a) = \frac{1}{L} \left| \{x \leq L : Z_x \equiv a \pmod m\} \right|.$$

Part (1) of the following proposition is in essence saying that the difference between $\Phi(L; m, a)$ and the expected value $1/m$ is not too large. Part (2) of the proposition is a high dimensional version of part (1), and part (3) is modeled on a slightly different situation under the same idea.

Proposition 3.1. *Let L be a positive integer.*

(1) *Let $\mathbf{v} = (v_1, \dots, v_L), \mathbf{v}' = (v'_1, \dots, v'_L) \in \mu_\ell^k$. Suppose $GCD(\ell, m) = 1$, then*

$$\sum_{a=0}^{m-1} \sum_{\mathbf{v},\mathbf{v}' \in \mu_\ell^L} \left| \sum_{x=1}^{L} \sum_{t=1}^{m-1} e_m \left(t \left(\sum_{j=1}^{x} F(v_j) - \sum_{j=1}^{x} F(v'_j) - a \right) \right) \right|^2 \leq 7m^4 L \ell^{2L+2}.$$

(2) *Let k be a positive integer and $\boldsymbol{a} = (a_1, \dots, a_k) \in (\mathbb{Z}/m\mathbb{Z})^k$. For $1 \leq l \leq k$, let $\mathbf{v}_l = (v_{l,1}, \dots, v_{l,L}), \mathbf{v}'_l = (v'_{l,1}, \dots, v'_{l,L}) \in \mu_\ell^L$. Suppose $GCD(\ell, m) = 1$, then*

$$\sum_{a \in (\mathbb{Z}/m\mathbb{Z})^k} \sum_{\substack{\mathbf{v}_l, \mathbf{v}'_l \in \mu_\ell^L \\ 1 \leq l \leq k}} \left| \sum_{x=1}^{L} \sum_{\mathbf{t}=(t_1,\dots,t_k) \neq \mathbf{0}} e_m \left(\sum_{l=1}^{k} t_l \left(\sum_{j=1}^{x} F(v_{l,j}) - \sum_{j=1}^{x} F(v'_{l,j}) - a_l \right) \right) \right|^2 \leq 7m^{2k+2} L \ell^{2Lk+2}.$$

(3) *If $\mathbf{v} = (v_1, \dots, v_L), \mathbf{v}' = (v'_1, \dots, v'_L) \in \{0,1\}^k$, then*

$$\sum_{a=0}^{m-1} \sum_{\mathbf{v},\mathbf{v}' \in \{0,1\}} \left| \sum_{x=1}^{L} \sum_{t=1}^{m-1} e_m \left(t \left(\sum_{j=1}^{x} v_j - \sum_{j=1}^{x} v'_j - a \right) \right) \right|^2 \leq 2^{2L+2} m^4 L.$$

Proof. (1) follows from (2) by taking $k = 1$. For (2), consider

$$\begin{aligned}
&\sum_{\mathbf{v}_l,\mathbf{v'}_l\in\mu_\ell^L}\left|\sum_{x=1}^{L}\sum_{\mathbf{t}\neq\mathbf{0}} e_m\left(\sum_{l=1}^{k} t_l\left(\sum_{j=1}^{x}F(v_{l,j})-\sum_{j=1}^{x}F(v'_{l,j})-a_l\right)\right)\right|^2\\
&=\sum_{\mathbf{v}_l,\mathbf{v'}_l\in\mu_\ell^L}\left(\sum_{x_1=1}^{L}\sum_{\mathbf{t}_1\neq\mathbf{0}} e_m\left(\sum_{l=1}^{k} t_{l,1}\left(\sum_{j=1}^{x_1}F(v_{l,j})-\sum_{j=1}^{x_1}F(v'_{l,j})-a_l\right)\right)\right)\\
&\qquad\times\left(\sum_{x_2=1}^{L}\sum_{\mathbf{t}_2\neq\mathbf{0}} e_m\left(-\sum_{l=1}^{k} t_{l,2}\left(\sum_{j=1}^{x_2}F(v_{l,j})-\sum_{j=1}^{x_2}F(v'_{l,j})-a\right)\right)\right)\\
&=\sum_{\mathbf{v}_l,\mathbf{v'}_l\in\mu_\ell^L}\sum_{1\le x_1,x_2\le L}\sum_{\mathbf{t}_1,\mathbf{t}_2\neq\mathbf{0}}\prod_{l=1}^{k} e_m(a_l(t_{l,2}-t_{l,1}))\\
&\qquad\times e_m\left(\sum_{l=1}^{k}\left(t_{l,1}\left(\sum_{j=1}^{x_1}F(v_{l,j})-\sum_{j=1}^{x_1}F(v'_{l,j})\right)-t_{l,2}\left(\sum_{j=1}^{x_2}F(v_{l,j})-\sum_{j=1}^{x_2}F(v'_{l,j})\right)\right)\right).
\end{aligned}\tag{3.5}$$

Here $\mathbf{t}_1 = (t_{1,1},\dots,t_{k,1})$, and similarly for $\mathbf{t}_2$.

We now sum over all a_l with $0 \le a_l \le m-1$ and use the orthogonality relation

$$\sum_{a_l=0}^{m-1} e_m(a_l(t_{l,2}-t_{l,1})) = \begin{cases} m, & t_{l,1}=t_{l,2},\\ 0, & t_{l,1}\neq t_{l,2}.\end{cases}$$

Then (3.5) becomes

$$\begin{aligned}
&m^k\sum_{\mathbf{v}_l,\mathbf{v'}_l\in\mu_\ell^L}\sum_{\mathbf{t}\neq\mathbf{0}}\sum_{1\le x_1,x_2\le L}\\
&\qquad e_m\left(\sum_{l=1}^{k} t_l\left(\sum_{j=1}^{x_1}F(v_{l,j})-\sum_{j=1}^{x_1}F(v'_{l,j})-\sum_{j=1}^{x_2}F(v_{l,j})+\sum_{j=1}^{x_2}F(v'_{l,j})\right)\right).
\end{aligned}$$

We separate the terms with $x_1 = x_2$ for which the looped sums inside the exponential vanish, which gives the total $m^k(m^k-1)L\ell^{2Lk}$. For the remaining terms, note that the looped sum for a particular pair is the negative of that of its reverse pair.

So the above sum is

$$\begin{aligned}
&m^k(m^k-1)L\ell^{2Lk} + m^k \sum_{\mathbf{t}\neq\mathbf{0}} \sum_{1\le x_1<x_2\le L} \sum_{\mathbf{v}_l,\mathbf{v'}_l\in\mu_\ell^L} \\
&\quad e_m\left(\sum_{l=1}^{k} t_l \left(\sum_{j=x_1+1}^{x_2} F(v_{l,j}) - \sum_{j=x_1+1}^{x_2} F(v'_{l,j})\right)\right) \\
&\quad + e_m\left(-t_l \left(\sum_{j=x_1+1}^{x_2} F(v_{l,j}) - \sum_{j=x_1+1}^{x_2} F(v'_{l,j})\right)\right) \\
=&m^k(m^k-1)L\ell^{2Lk} + 2m^k \sum_{\mathbf{t}\neq\mathbf{0}} \sum_{1\le x_1<x_2\le L} \\
&\ell^{2Lk-2k(x_2-x_1)} \prod_{l=1}^{k} (e_m(\ell t_l)+\ell-1)^{x_2-x_1}(e_m(-\ell t_l)+\ell-1)^{x_2-x_1} \\
=&m^k(m^k-1)L\ell^{2Lk} \\
&+ 2m^k\ell^{2Lk} \sum_{\mathbf{t}\neq\mathbf{0}} \sum_{1\le x_1<x_2\le L} \prod_{l=1}^{k} \left(\frac{(e_m(\ell t_l)+\ell-1)(e_m(-\ell t_l)+\ell-1)}{\ell^2}\right)^{x_2-x_1}, \qquad (3.6)
\end{aligned}$$

where in the penultimate step, we used

$$\sum_{v^\ell=1} e_m(tF(v)) = e_m(\ell t)+\ell-1.$$

For $GCD(\ell, m) = 1$, we have

$$\left|\cos\left(\frac{2\pi\ell t}{m}\right)\right| \le 1 - \frac{\pi^2}{3m^2}$$

for any $1 \le t \le m-1$. Hence,

$$\begin{aligned}
\frac{(e_m(\ell t)+\ell-1)(e_m(-\ell t)+\ell-1)}{\ell^2} &= \frac{\ell^2-2\ell+2+2(\ell-1)\cos\frac{2\pi\ell t}{m}}{\ell^2} \\
&\le 1 - \frac{2(\ell-1)(1-\frac{\pi^2}{3m^2})}{\ell^2}. \qquad (3.7)
\end{aligned}$$

Fix $x_2 - x_1 = d$. For each $1 \le d \le L-1$, the number of (x_1, x_2) with $1 \le x_1 < x_2 \le L$ with $x_2 - x_1 = d$ is $L - d$. So (3.7) implies

$$\begin{aligned}
&\sum_{1\le x_1<x_2\le L} \left(\frac{(e_m(\ell t)+\ell-1)(e_m(-\ell t)+\ell-1)}{\ell^2}\right)^{x_2-x_1} \\
\le&\sum_{d=1}^{L-1}(L-d)\left(1-\frac{2(\ell-1)(1-\frac{\pi^2}{3m^2})}{\ell^2}\right)^d \\
\le&3m^2\ell^2 L
\end{aligned}$$

after some simplification. For any $\mathbf{t} \neq \mathbf{0}$ we have a nonzero coordinate for which the above calculations apply. Thus

$$\sum_{\mathbf{t}\neq\mathbf{0}} \sum_{1\le x_1<x_2\le L} \prod_{l=1}^{k} \left(\frac{(e_m(\ell t_l)+\ell-1)(e_m(-\ell t_l)+\ell-1)}{\ell^2} \right)^{x_2-x_1} \le (m^k-1)(3m^2\ell^2 L).$$

Part (2) now follows easily by inserting the above estimate in (3.6).

For (3), we derive as above that

$$\begin{aligned} (3.8)\qquad & \sum_{\mathbf{v},\mathbf{v}'\in\mu_\ell^L} \left| \sum_{x=1}^{L} \sum_{t=1}^{m-1} e_m\left(t\left(\sum_{j=1}^{x} v_j - \sum_{j=1}^{x} v_j' - a \right)\right)\right|^2 \\ &= m(m-1)2^{2L}L + m\sum_{t=1}^{m-1} \sum_{1\le x_1<x_2\le L} \sum_{\mathbf{v},\mathbf{v}'\in\{0,1\}} e_m\left(t\left(\sum_{j=x_1+1}^{x_2} v_j - \sum_{j=x_1+1}^{x_2} v_j' \right)\right) \\ &\qquad + e_m\left(-t\left(\sum_{j=x_1+1}^{x_2} v_j - \sum_{j=x_1+1}^{x_2} v_j' \right)\right). \end{aligned}$$

Here from

$$\sum_{v\in\{0,1\}} e_m(tv) = 1 + e_m(t)$$

and the inequality

$$\left|\cos\left(\cos\frac{\pi t}{m}\right)\right| \le 1 - \frac{\pi^2}{3m^2},$$

we see that the second term in (3.8) is

$$\begin{aligned} & 2\cdot 2^{2L} m \sum_{t=1}^{m-1} \sum_{1\le x_1<x_2\le L} \left(\frac{(1+e_m(t))(1+e_m(-\ell t))}{4} \right)^{x_2-x_1} \\ =& 2^{2L+1} m^2 \sum_{d=1}^{L-1} (L-d) \left(\cos\frac{\pi t}{m}\right)^d \\ \le& 2^{2L+1} m^2 L \sum_{d=1}^{L-1} \left(1-\frac{\pi^2}{3m^2}\right)^d \\ =& 2^{2L+1} m^2 L \left(1-\frac{\pi^2}{3m^2}\right) \frac{1-\left(1-\frac{\pi^2}{3m^2}\right)^{2L-2}}{\frac{\pi^2}{3m^2}} \\ \le& 2^{2L+1} m^4 L. \end{aligned}$$

Substituting this back into (3.8) completes the proof of (3).

□

The next lemma is the classical Weil bound for incomplete exponential sums over $\mathbb{F}_p$. Let χ_ℓ be a nontrivial multiplicatively character of order ℓ. For a polynomial $P(x) \in \mathbb{F}_p[x]$ of degree d and an interval $\mathcal{I} \subseteq [0, p-1]$, define

$$S_{\mathcal{I}}(P) = \sum_{x\in\mathcal{I}} \chi_\ell(P(x)).$$

Lemma 3.3. *If $P(x)$ is not a complete ℓ-th power, then*

$$|S_{\mathcal{I}}(P)| \leq 2(d+1)\sqrt{p}\log p.$$

Proof. If $\mathcal{I}$ is the complete interval $[0, p-1]$, the result follows from Weil's estimate [27]. The same estimate hold for the sum:

$$\left|\sum_{x\in[0,p-1]} \chi_\ell(P(x))e_p(-tx)\right| \leq (d+1)\sqrt{p} \tag{3.9}$$

for any $t \in \mathbb{F}_p$. If $\mathcal{I}$ is not the complete interval, let $\mathcal{I} \cap \mathbb{Z} = \{a, a+1, \dots, b\}$. We use a standard method to express the incomplete sum $S_{\mathcal{I}}(P)$ in terms of complete sums. More precisely, we have

$$S_{\mathcal{I}}(P) = \sum_{x\in[0,p-1]} \chi_\ell(P(x)) \left(\frac{1}{p}\sum_{n\in\mathcal{I}}\sum_{t \bmod p} e_p(t(n-x))\right).$$

Changing the order of summation and using (3.9), we get

$$\begin{aligned}
|S_{\mathcal{I}}(P)| &= \left|\frac{1}{p}\sum_{t \bmod p}\left(\sum_{n\in\mathcal{I}} e_p(tn)\right)\left(\sum_{x\in[0,p-1]} \chi_\ell(P(x))e_p(-tx)\right)\right| \\
&\leq \frac{1}{p}(d+1)\sqrt{p}\left|\sum_{t \bmod p}\left(\sum_{n\in\mathcal{I}} e_p(tn)\right)\right| \\
&= \frac{1}{p}(d+1)\sqrt{p}\left(|\mathcal{I}| + \left|\sum_{t\neq 0 \bmod p} \frac{e_p(t(a+1)) - e_p(t(b+1))}{1-e_p(t)}\right|\right) \\
&= \frac{1}{p}(d+1)\sqrt{p}\left(|\mathcal{I}| + \sum_{t\neq 0 \bmod p} \frac{1}{|\sin(t\pi/p)|}\right). \qquad (3.10)
\end{aligned}$$

Since $|\sin(t\pi/p)| \geq \frac{\pi|t|}{2p}$, we obtain

$$\sum_{t\neq 0 \bmod p} \frac{1}{|\sin(t\pi/p)|} \leq 2\sum_{t=1}^{\frac{p-1}{2}} \frac{2p}{\pi\,|t|} \leq \frac{4}{\pi}p\log p.$$

Inserting the above estimate into (3.10), we obtain

$$|S_{\mathcal{I}}(P)| \leq \frac{1}{p}(d+1)\sqrt{p}(|\mathcal{I}| + \frac{4}{\pi}p\log p) \leq 2(d+1)\sqrt{p}\log p.$$

This finishes the proof of the lemma. □

4. Distribution of the number of points in residue classes: proof of Theorem 1

Recall that we are studying the curve

$$\mathcal{C}: \qquad y^\ell = P(x).$$

We defined the quantities

$$N_{\mathcal{C}}(x_0, I) = \#\{(x,y) \in \mathcal{C}(\mathbb{F}_p) : x_0 < x \leq x_0 + I\},$$

which is the number of points on $\mathcal{C}$ inside a rectangle of some fixed length I, and

$$\Phi_{\mathcal{C}}(m,a)=\frac{1}{|\mathcal{I}|}\#\{0\le x_0\le p-1: N_{\mathcal{C}}(x_0,I)\equiv a \mod m\},$$

which can be regarded as the probability of the occurrence of $N_{\mathcal{C}}(x_0,I)\equiv a \mod m$ for $x_0\in\mathcal{I}$.

Let N be a large number, $x_1,\dots,x_r\in\mathbb{F}_p$ be distinct points and let $\mathbf{x}=(x_1,\dots,x_r)$. Let $P(x)\in\mathbf{F}_p$ be a polynomial of degree d, and $\mathbf{v}=(v_1,\dots,v_r)\in\mu_\ell^r$. Suppose $L\neq 0$ is an integer, and define

$$M_P(\mathbf{v})=M_{P,r,N,k}(\mathbf{v},\mathbf{x})=\{0\le i\le N:\chi_\ell(P(iL+x_j))=v_j\ \forall 1\le j\le r\}. \tag{4.1}$$

This will serve as our bridge between the character values and the random walk setting. The following proposition estimates the size of $M_P(\mathbf{v})$.

Proposition 4.1. *If $r<(\log p)/\log(4d)$ and $P(x)$ is not a complete ℓ-th power, then for any $\mathbf{v}\in\mu_\ell^r$, we have*

$$\#M_P(\mathbf{v})=\frac{N}{\ell^r}+\frac{2(dr(\ell-1)+1)}{\ell^r}\sqrt{p}\log p+O(d).$$

Proof. The number of points $x\in\mathbb{F}_p$ with $P(x)=0$ is $O(\deg P)=O(d)$. Hence, there are $N+O(d)$ indices i such that $P(iL+x_j)\neq 0$ for all $1\le j\le r$. For those i, we have

$$\frac{1}{\ell^r}\prod_{j=1}^{r}F(v_j^{-1}\chi_\ell(P(iL+x_j)))=\begin{cases}1 & \text{, if } i\in M_P(\mathbf{v}),\\ 0 & \text{, otherwise,}\end{cases}$$

where $F(v)$ is defined in (3.4). Thus,

$$\#M_P(\mathbf{v})=\frac{1}{\ell^r}\sum_{i=0}^{N}\prod_{j=1}^{r}F(v_j^{-1}\chi_\ell(P(iL+x_j)))+O(d).$$

Expanding the above product and changing the order of summation, we obtain

$$\begin{aligned}\#M_P(\mathbf{v})=\frac{N}{\ell^r}+\frac{1}{\ell^r}\sum_{\substack{\mathbf{e}=(e_1,\dots,e_r)\neq 0\\ 0\le e_j\le \ell-1}} & v_1^{-e_1}\dots v_r^{-e_r}\\ &\times\sum_{i=0}^{N}\chi_\ell(P(iL+x_1))^{e_1}\dots\chi_\ell(P(iL+x_r))^{e_r}+O(d).\end{aligned} \tag{4.2}$$

Since the x_j are distinct points on $\mathbb{F}_p$ and $r<(\log p)/\log(4\deg P)$, Lemma 3.2 shows that the polynomial

$$Q(i)=P(iL+x_1)^{e_1}\dots P(iL+x_r)^{e_r}$$

is not a complete ℓ-th power. Hence, by Lemma 3.3, we have

$$\left|\sum_{i=1}^{N}\chi_\ell\left(P(iL+x_1)^{e_1}\dots P(iL+x_r)^{e_r}\right)\right|\le 2(dr(\ell-1)+1)\sqrt{p}\log p.$$

Inserting the above estimate back into (4.2), we obtain

$$\#M_P(\mathbf{v})\le\frac{N}{\ell^r}+\frac{2(dr(\ell-1)+1)}{\ell^r}\sqrt{p}\log p+O(d).$$

□

We are now ready to prove Theorem 1.

Proof of Theorem 1. Let $L = L(p) \leq \left[\frac{\log p}{2\log 4d}\right]$ be a large number, and let $N = [|\mathcal{I}|/L] - 1$. Define

$$R_{P,m,a}(i,L) = \#\{1 \leq x \leq L : N_{\mathcal{C}}(iL+x, I) \equiv a \pmod m\}.$$

We have

$$\left|\Phi_{\mathcal{C}}(m,a) - \frac{1}{m}\right| \leq \frac{1}{|\mathcal{I}|}\sum_{i=0}^{N}\left|R_{P,m,a}(i,L) - \frac{L}{m}\right| + O\left(\frac{L}{|\mathcal{I}|}\right). \tag{4.3}$$

By the Cauchy-Schwarz inequality,

$$\left(\sum_{i=0}^{N}\left|R_{P,m,a}(i,L) - \frac{L}{m}\right|\right)^2 \leq (N+1)\sum_{i=0}^{N}\left(R_{P,m,a}(i,L) - \frac{L}{m}\right)^2.$$

Putting this back into (4.3), we obtain

$$\left(\Phi_{\mathcal{C}}(m,a) - \frac{1}{m}\right)^2 \leq \frac{N+1}{|\mathcal{I}|^2}\sum_{i=0}^{N}\left(R_{P,m,a}(i,L) - \frac{L}{m}\right)^2 + O\left(\frac{L^2}{|\mathcal{I}|^2}\right). \tag{4.4}$$

Now note that

$$N_{\mathcal{C}}(iL+x, I) = N_{\mathcal{C}}(iL, I) + \sum_{j=1}^{x} F(\chi_\ell(P(iL+I+j))) - \sum_{j=1}^{x} F(\chi_\ell(P(iL+j))),$$

so if we set

$$R'_{P,m,b}(i,L) = \frac{1}{m}\#\{1 \leq x \leq L : \sum_{j=1}^{x} F(\chi_\ell(P(iL+I+j))) - \sum_{j=1}^{x} F(\chi_\ell(P(iL+j))) \equiv b \pmod m\}$$

and use the substitution $b = a + N_{\mathcal{C}}(sL, I)$, then

$$\sum_{a=0}^{m-1}\sum_{i=0}^{N}\left(R_{P,m,a}(i,L) - \frac{L}{m}\right)^2 = \sum_{b=0}^{m-1}\sum_{i=0}^{N}\left(R'_{P,m,b}(i,L) - \frac{L}{m}\right)^2. \tag{4.5}$$

Using the orthogonality of character sums, we get

$$R'_{P,m,b}(i,L) = \sum_{x=1}^{L}\sum_{t=0}^{m-1} e_m\left(t\left(\sum_{i=1}^{x} F(\chi_\ell(P(iL+I+j)) - \sum_{i=1}^{x} F(\chi_\ell(P(iL+j)) - b\right)\right),$$

and hence

$$\begin{aligned}
&\sum_{i=0}^{N}\left(R'_{P,m,b}(i,L)-\frac{L}{m}\right)^2\\
=&\frac{1}{m^2}\sum_{i=0}^{N}\left|\sum_{x=1}^{L}\sum_{t=0}^{m-1}e_m\left(t\left(\sum_{j=1}^{x}F(\chi_\ell(P(iL+I+j))-\sum_{j=1}^{x}F(\chi_\ell(P(iL+j))-b\right)-L\right)\right|^2\\
=&\frac{1}{m^2}\sum_{i=0}^{N}\left|\sum_{x=1}^{L}\sum_{t=1}^{m-1}e_m\left(t\left(\sum_{j=1}^{x}F(\chi_\ell(P(iL+I+j))-\sum_{j=1}^{x}F(\chi_\ell(P(iL+j))-b\right)\right)\right|^2\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad(4.6)\\
=&\frac{1}{m^2}\sum_{\mathbf{v},\mathbf{v}'\in\mu_\ell^L}\left|\sum_{x=1}^{L}\sum_{t=1}^{m-1}e_m\left(t\left(\sum_{j=1}^{x}F(v_j)-\sum_{j=1}^{x}F(v'_j)-b\right)\right)\right|^2\cdot\#M_P(\mathbf{w}),
\end{aligned}$$

where $M_P(\mathbf{w})$ is defined in (4.1), with $\mathbf{v}=(v_1,\dots,v_L)$, $\mathbf{v}'=(v'_1,\dots,v'_L)$, $\mathbf{w}=(v_1,\dots,v_L,v'_1,\dots,v'_L)$, and

$$\mathbf{x}=(iL+I+1,\dots,iL+I+L,iL+1,\dots,iL+L).$$

Note that as $p-L>I>L$, the entries in $\mathbf{x}$ are indeed distinct. Putting (4.6) back into (4.5), applying Proposition 3.1(1) and Proposition 4.1, we have after some simplifications

$$\sum_{a=0}^{m-1}\sum_{i=0}^{N}\left(R_{P,m,a}(i,L)-\frac{L}{m}\right)^2=\frac{7m^3\ell^2LN^2}{|\mathcal{I}|^2}+O\left(\frac{m^3\ell^3L^2N\sqrt{p}\log p}{|\mathcal{I}|^2}\right).$$

Combining this estimate with (4.4), we obtain

$$\sum_{a=0}^{m-1}\left(\Phi_{\mathcal{C}}(m,a)-\frac{1}{m}\right)^2\le\frac{7m^3\ell^2}{L}+O\left(\frac{m^3\ell^3L\sqrt{p}\log p}{|\mathcal{I}|}\right).$$

This completes the proof of Theorem 1. □

5. Joint distribution among curves: proof of Theorem 2

Before we prove Theorem 2, we need a generalization of Proposition 4.1. Let $x_1,\dots,x_r\in\mathbb{F}_p$ be distinct points, and let $\mathbf{x}=(x_1,\dots,x_r)$. For $1\le l\le k$, let $P_l(x)\in\mathbf{F}_p$ be polynomials of degree d_l, $d=d_1+\dots+d_k$, and $\mathbf{v}_l=(v_{l,1},\dots,v_{l,r})\in\mu_\ell^r$. Suppose $L\neq0$ is an integer, and define the set

$$M_{P_1,\dots,P_k}(\mathbf{v}_1,\dots,\mathbf{v}_k)=\{0\le i\le N:\chi_\ell(P_l(iL+x_j))=v_{l,j}\ \forall 1\le j\le r,1\le l\le k\}.$$

Proposition 5.1. *Assume the $P_l(x)$ are not complete ℓ-th powers, and the set $\{P_1(x),\dots,P_k(x)\}$ is multiplicatively independent. If $r<(\log p)/\log(4d)$, then for any $\mathbf{v}_1,\dots,\mathbf{v}_k$, we have*

$$\#M_{P_1,\dots,P_k}(\mathbf{v}_1,\dots,\mathbf{v}_k)=\frac{N}{\ell^{kr}}+\frac{2dkr(\ell-1)+1}{\ell^{kr}}\sqrt{p}\log p+O(d).$$

Proof. We follow the same idea as in the proof of Proposition 4.1. For those $x \in \mathbb{F}_p$ which are not roots of any P_l, we have

$$\frac{1}{\ell^{kr}} \prod_{l=1}^{k} \prod_{j=1}^{r} F(v_j^{-1} \chi_\ell(P_l(iL + x_j))) = \begin{cases} 1 & , \text{ if } i \in M_{P_1,\dots,P_k}(\mathbf{v}_1, \dots, \mathbf{v}_k), \\ 0 & , \text{ otherwise.} \end{cases}$$

So,

$$\#M_{P_1,\dots,P_k}(\mathbf{v}_1, \dots, \mathbf{v}_k) = \frac{1}{\ell^{kr}} \sum_{i=0}^{N} \prod_{l=1}^{k} \prod_{j=1}^{r} F(v_j^{-1} \chi_\ell(P_l(iL + x_j))) + O(d).$$

Expanding the above product, we obtain

$$\begin{aligned} \#M_{P_1,\dots,P_k}(\mathbf{v}_1, \dots, \mathbf{v}_k) = \frac{N}{\ell^{kr}} + \frac{1}{\ell^{kr}} \sum_{\mathbf{e} \in S} \prod_{l=1}^{k} \prod_{j=1}^{r} v_{l,j}^{-e_{l,j}} \\ \times \sum_{i=0}^{N} \chi_\ell \left(\prod_{l=1}^{k} \prod_{j=1}^{r} P_l(iL + x_r) \right)^{e_{l,r}} + O(d), \end{aligned} \tag{5.1}$$

where

$$S = \{\mathbf{e} = (e_{l,j})_{\substack{1 \le l \le k \\ 1 \le j \le r}} : 0 \le e_{l,j} \le \ell - 1\}.$$

As $r < (\log p)/\log(4d)$ and the P_l's are multiplicatively independent, Lemma 3.2 implies that the polynomial

$$Q(i) = \prod_{l=1}^{k} \prod_{j=1}^{r} P_l(iL + x_r)^{e_{l,r}}$$

cannot be a complete ℓ-th power for any choice of $\mathbf{e} \in S$ unless $\mathbf{e}$ is the zero vector. Therefore, we can employ Lemma 3.3 in (5.1) to get

$$\#M_{P_1,\dots,P_k}(\mathbf{v}_1, \dots, \mathbf{v}_k) = \frac{N}{\ell^{kr}} + \frac{2(dkr(\ell - 1) + 1)}{\ell^{kr}} \sqrt{p} \log p + O(d).$$

□

Proof of Theorem 2. The proof of Theorem 2 follows the same line as that of Theorem 1. Let $L = L(p) \le \left[\frac{\log p}{2 \log 4d} \right]$, and let $N = [|\mathcal{I}|/L] - 1$. Define

$$R_{m,\mathbf{a},k}(i, L) = \#\{1 \le x \le L : N_l(iL + x, I) \equiv a_l \pmod m \ \forall 1 \le l \le k\}.$$

We have

$$\left| \Phi(m, \mathbf{a}) - \frac{1}{m^k} \right| \le \frac{1}{|\mathcal{I}|} \sum_{i=0}^{N} \left| R_{m,\mathbf{a},k}(i, L) - \frac{L}{m^k} \right| + O\left(\frac{L}{p} \right).$$

Again by Cauchy-Schwarz inequality,

$$\left(\sum_{i=0}^{N} \left| R_{m,\mathbf{a},k}(i, L) - \frac{L}{m^k} \right| \right)^2 \le (N + 1) \sum_{i=0}^{N} \left(R_{m,\mathbf{a},k}(i, L) - \frac{L}{m^k} \right)^2,$$

which implies

$$\left| \Phi(m, \mathbf{a}) - \frac{1}{m^k} \right|^2 \le \frac{N + 1}{|\mathcal{I}|^2} \sum_{i=0}^{N} \left(R_{m,\mathbf{a},k}(i, L) - \frac{L}{m^k} \right)^2 + O\left(\frac{L^2}{p^2} \right).$$

Note that

$$N_l(iL+x,I) = N_l(iL,I) + \sum_{j=1}^{x} F(\chi_\ell(P_l(iL+I+j))) - \sum_{j=1}^{x} F(\chi_\ell(P_l(iL+j)))$$

for all $1 \le l \le k$. To simplify the notations, write

$$\Sigma(x,l) = \sum_{j=1}^{x} F(\chi_\ell(P_l(iL+I+j))) - \sum_{j=1}^{x} F(\chi_\ell(P_l(iL+j))).$$

Let $\mathbf{b} = \mathbf{a} + (N_l(sL,I))_{1\le l\le k}$, and set

$$R'_{m,\mathbf{b}}(i,L) = \#\{1 \le x \le L : \Sigma(x,l) \equiv b_l \pmod m \ \forall 1 \le l \le k\},$$

then

$$\sum_{a\in(\mathbb{Z}/m\mathbb{Z})^k} \sum_{i=0}^{N} \left(R_{m,\mathbf{a}}(i,L) - \frac{L}{m^k}\right)^2 = \sum_{b\in(\mathbb{Z}/m\mathbb{Z})^k} \sum_{i=0}^{N} \left(R'_{m,\mathbf{b}}(i,L) - \frac{L}{m^k}\right)^2. \tag{5.2}$$

Since

$$R'_{m,\mathbf{b}}(i,L) = \frac{1}{m^k} \sum_{x=1}^{L} \prod_{l=1}^{k} \sum_{t_l=0}^{m-1} e_m(t_l\Sigma(x,l) - b_l),$$

a similar calculation as in (4.6) gives

$$\begin{aligned}
&\sum_{i=0}^{N} \left(R'_{m,\mathbf{b}}(i,L) - \frac{L}{m^k}\right)^2 \\
=&\frac{1}{m^{2k}} \sum_{i=0}^{N} \left| \sum_{x=1}^{L} \prod_{l=1}^{k} \sum_{t_l=0}^{m-1} e_m(t_l\Sigma(x,l) - b_l) - L \right|^2 \\
=&\frac{1}{m^{2k}} \sum_{\mathbf{v}_l,\mathbf{v}'_l\in\mu_\ell^L} \left| \sum_{x=1}^{L} \sum_{\mathbf{t}\neq\mathbf{0}} e_m\left(\sum_{l=1}^{k} t_l \left(\sum_{j=1}^{x} F(v_{l,j}) - \sum_{j=1}^{x} F(v'_{l,j}) - b_l\right)\right)\right|^2 \\
&\times \#M_{P_1,\dots,P_k}(\mathbf{w}_1,\dots,\mathbf{w}_k),
\end{aligned} \tag{5.3}$$

with $\mathbf{w}_l = (\mathbf{v}_l, \mathbf{v}'_l)$. Substituting (5.3) back into (5.2), applying Proposition 3.1(2) and Proposition 5.1, we obtain

$$\sum_{\mathbf{a}\in(\mathbb{Z}/m\mathbb{Z})^k} \sum_{i=0}^{N} \left(R'_{m,\mathbf{b}}(i,L) - \frac{L}{m^k}\right)^2 \le 7NLm^{k+2}\ell^2 + O(dkL^2\ell^3 m^{k+2}\sqrt{p}\log p),$$

and so

$$\sum_{\mathbf{a}\in(\mathbb{Z}/m\mathbb{Z})^k} \left(\Phi(m,\mathbf{a}) - \frac{1}{m^k}\right)^2 \le \frac{7m^{k+2}\ell^2}{L} + O\left(\frac{dkL\ell^3 m^{k+2}\sqrt{p}\log p}{|\mathcal{I}|}\right).$$

□

6. The case of restricted domains: proof of Theorem 3

In this section we study the case when the domain is restricted to a smaller rectangle $\Omega = \mathcal{I} \times \mathcal{J}$ that satisfies the condition $(*)$. For any $x \in [0, p-1]$, define

$$\delta_{\mathcal{C},\Omega}(x) = \begin{cases} 1 & , \text{ if } x \in \mathcal{I} \text{ and } \exists y \in \mathcal{J} \text{ so that } (x,y) \in \mathcal{C}, \\ 0 & , \text{ otherwise.} \end{cases}$$

Let $\mathbf{x} = (x_1, \dots, x_r) \in [0, p-1]^r$, and let $\mathbf{v} = (v_1, \dots, v_r) \in \{0,1\}^r$ be a vector. As in the proofs of previous theorems, we introduce a set and estimate its size. Define

$$M_{\mathcal{C},\Omega}(\mathbf{v}) = \{x \in \mathcal{I} : L|x, \delta_{\mathcal{C},\Omega}(x + x_j) = v_j \ \forall 1 \le j \le r\}.$$

Remark 6.1. For $x \in \mathcal{I}$, one can write down an explicit formula for $\delta_{\mathcal{C},\Omega}(x)$ involving exponential sums. Write the defining equation of $\mathcal{C}$ as $f(x,y) := y^\ell - P(x) = 0$. Consider

$$S(x) = \sum_{y \in \mathcal{J}} \sum_{t \in \mathbb{F}_p} t f(x,y).$$

Then S is the number of points in $\mathcal{C} \cap \Omega$. Now our assumption $(*)$ guarantees that $\delta_{\mathcal{C},\Omega}(x) = S(x)$. This formula was used by Dwork [10] to prove the rationality of zeta functions of varieties over finite fields. We will not need this formula in our paper.

In previous sections, we used characters to relate the random walk setting and the distribution of number of points on $\mathcal{C}$, which does not allow us to control the y-coordinates. To allow restrictions on the domain, we proceed as follows. Let $\mathcal{H} = \{h_1, \dots, h_r\} \subseteq [0, p-1]$ be a set of integers. From the curve $\mathcal{C}$ defined by (1.1), we construct the *x-shifted curve* $\mathcal{C}_\mathcal{H}$ to be the curve defined by the following system of equations:

$$\begin{aligned} y_1^\ell &= P(x + h_1) \\ y_2^\ell &= P(x + h_2) \\ &\vdots \\ y_r^\ell &= P(x + h_r). \end{aligned}$$

It is easy to see that $\mathcal{C}_\mathcal{H}$ is indeed a curve. The next lemma shows that this curve is absolutely irreducible if r is not too large.

Lemma 6.1. *If $r < \frac{\log p}{\log(4d)}$, then $\mathcal{C}_\mathcal{H}$ is absolutely irreducible.*

Proof. It suffices to show that for any $\mathbf{e} = (e_1, \dots, e_r)$ with $0 \le e_j \le \ell - 1$, $\mathbf{e} \ne 0$, the combination

$$Q(x) = \prod_{j=1}^{r} P(x + h_j)^{e_j}$$

cannot be a complete ℓ-th power, and this is shown in Lemma 3.2. □

Let $\Omega = \mathcal{I} \times \mathcal{J} \subseteq [0, p-1]^2$ be a rectangle, and let $N_{\mathcal{C},\Omega}(\mathcal{H})$ be the number of points on $\mathcal{C}_\mathcal{H}$ inside Ω with $L|x$. Since $\mathcal{C}_\mathcal{H}$ is absolutely irreducible, we can determine $N_{\mathcal{C},\Omega}(\mathcal{H})$ using the idea of generalized Lehmer problem on curves [7]. In particular, we have

$$N_{\mathcal{C},\Omega}(\mathcal{H}) = \frac{|\mathcal{I}|}{L} \cdot \frac{|\mathcal{J}|^{|\mathcal{H}|}}{p^{|\mathcal{H}|}} + O(\sqrt{p} \log^{|\mathcal{H}|+1} p),$$

where $|\mathcal{I}| = \#(\mathcal{I} \cap \mathbb{Z})$. Note that $N_{\mathcal{C},\Omega}(\mathcal{H})$ only depends on the cardinality of $\mathcal{H}$ but not the particular elements in it. Suppose now Ω satisfies $(*)$, then it is easy to see that

$$N_{\mathcal{C},\Omega}(\mathcal{H}) = \sum_{x \in \mathcal{I}, L|x} \prod_{h \in \mathcal{H}} \delta_{\mathcal{C},\Omega}(x+h).$$

Thus, if

$$\#\{x + x_r : x \equiv 0 \pmod{L}, x + x_r \notin \mathcal{I}\} = O(\sqrt{p}), \tag{6.1}$$

then we can estimate $M_{\mathcal{C},\Omega}(\mathbf{v})$ using $N_{\mathcal{C},\Omega}(\mathcal{H})$ by a combinatorial argument as follows. Divide the x_j's into two disjoint sets according to the corresponding values of v_j, say

$$\mathcal{A} = \{x_j : v_j = 1\} \qquad \text{and} \qquad \mathcal{B} = \{x_l : v_l = 0\}. \tag{6.2}$$

Then

$$\begin{aligned}
\#M_{\mathcal{C},\Omega}(\mathbf{v}) &= \sum_{x \in \mathcal{I}, L|x} \prod_{x_j \in \mathcal{A}} \delta(x+x_j) \prod_{x_l \in \mathcal{B}} (1 - \delta(x+x_l)) + O(\sqrt{p}) \\
&= \sum_{x \in \mathcal{I}, L|x} \prod_{x_j \in \mathcal{A}} \delta(x+x_j) \sum_{\mathcal{E} \subset \mathcal{B}} (-1)^{|\mathcal{E}|} \prod_{x_l \in \mathcal{E}} \delta(x+x_l) + O(\sqrt{p}) \\
&= \sum_{\mathcal{E} \subset \mathcal{B}} (-1)^{|\mathcal{E}|} \sum_{x \in \mathcal{I}, L|x} \prod_{x_j \in \mathcal{A} \cup \mathcal{E}} \delta(x+x_j) + O(\sqrt{p}) \\
&= \sum_{\mathcal{E} \subset \mathcal{B}} (-1)^{|\mathcal{E}|} N_{\mathcal{C},\Omega}(\mathcal{A} \cup \mathcal{E}) + O(\sqrt{p}) \\
&= \sum_{\mathcal{E} \subset \mathcal{B}} (-1)^{|\mathcal{E}|} \frac{|\mathcal{I}|}{L} \cdot \frac{|\mathcal{J}|^{|\mathcal{A}|+|\mathcal{E}|}}{p^{|\mathcal{A}|+|\mathcal{E}|}} + O(\sqrt{p} \log^{|\mathcal{A}|+|\mathcal{E}|+1} p) \\
&= \frac{|\mathcal{I}|}{L} \cdot \left(\frac{|\mathcal{J}|}{p}\right)^{|\mathcal{A}|} \left(1 - \frac{|\mathcal{J}|}{p}\right)^{|\mathcal{B}|} + O(2^r \sqrt{p} \log^{r+1} p).
\end{aligned}$$

We summarize the above results in the following proposition.

Proposition 6.1. *Suppose the domain $\mathcal{I} \times \mathcal{J}$ satisfies $(*)$, and let $\mathbf{x} = (x_1, \dots, x_r) \in [0, p-1]^r$ such that (6.1) is satisfied. Then for any $\mathbf{v}_1, \dots, \mathbf{v}_k$, we have*

$$\#M_{\mathcal{C},\Omega}(\mathbf{v}) = \frac{|\mathcal{I}|}{L} \cdot \left(\frac{|\mathcal{J}|}{p}\right)^{|\mathcal{A}|} \left(1 - \frac{|\mathcal{J}|}{p}\right)^{|\mathcal{B}|} + O(2^r \sqrt{p} \log^{r+1} p),$$

where $\mathcal{A}$ and $\mathcal{B}$ is as in (6.2). In particular,

$$\#M_{\mathcal{C},\Omega}(\mathbf{v}) \le \frac{|\mathcal{I}|}{2^r L} + O(2^r \sqrt{p} \log^{r+1} p).$$

Note that the above proposition is meaningful only when the main term is larger than the error term, hence we need the conditions on $\mathcal{I}$, $\mathcal{J}$ as stated in Theorem 3. We are now ready to prove Theorem 3.

Proof of Theorem 3. Let L be a large integer of order $o(\log p / \log\log p)$, and $N = [p/L] - 1$. Define

$$R_{\mathcal{C},\Omega,m,a}(i, L) = \#\{1 \le x \le L : N_{\mathcal{C},\Omega}(iL + x, I) \equiv a \pmod{m}\}$$

and

$$R'_{\mathcal{C},\Omega,m,b}(i,L) = \#\{1 \le x \le L : \sum_{j=1}^{x} \delta_{\mathcal{C},\Omega}(iL+I+j) - \sum_{j=1}^{x} \delta_{\mathcal{C},\Omega}(iL+j) \equiv b \pmod m \quad \forall 1 \le l \le k\}.$$

Following a similar calculation as in the proof of Theorem 1 and Theorem 2, we arrive at

$$\sum_{a=0}^{m-1} \left(\Phi_{\mathcal{C},\Omega}(m,a) - \frac{1}{m}\right)^2 \le \frac{N+1}{p^2} \sum_{a=0}^{m-1}\sum_{i=0}^{N} \left(R_{\mathcal{C},\Omega,m,a}(i,L) - \frac{L}{m}\right)^2 + O\left(\frac{L}{p}\right)$$

$$= \frac{N+1}{p^2} \sum_{b=0}^{m-1}\sum_{i=0}^{N} \left(R'_{\mathcal{C},\Omega,m,b}(i,L) - \frac{L}{m}\right)^2 + O\left(\frac{L}{p}\right), \tag{6.3}$$

and

$$\sum_{i=0}^{N} \left(R'_{\mathcal{C},\Omega,m,b}(i,L) - \frac{L}{m}\right)^2 = \frac{1}{m^2} \left| \sum_{\mathbf{v},\mathbf{v}' \in \{0,1\}^L} \sum_{x=1}^{L}\sum_{t=1}^{m-1} e_m\left(t\left(\sum_{j=1}^{x} F(v_j) - \sum_{j=1}^{x} F(v'_j) - b\right)\right)\right|^2 \times \#M_{\mathcal{C},\Omega}(\mathbf{w}), \tag{6.4}$$

where $\mathbf{w} = (\mathbf{v}, \mathbf{v}')$. This time $\mathbf{x} = (iL+I+1, \dots, iL+I+L, iL+1, \dots, iL+L)$, and the condition $p - L > I > L$ guarantees that the entries in $\mathbf{x}$ are disjoint. Applying Proposition 3.1(3) and Proposition 6.1 to (6.4), we obtain

$$\sum_{b=0}^{m-1}\sum_{i=0}^{N} \left(R'_{\mathcal{C},\Omega,m,b}(i,L) - \frac{L}{m}\right)^2 \le 2^{2L+2} m^4 L \left(\frac{|\mathcal{I}|}{2^{2L}L} + O(2^{2L}\sqrt{p}\log^{2L+1} p)\right) \le 4m^4 |\mathcal{I}| + O(m^4 p^{\frac{1}{2}+\varepsilon})$$

for any $\varepsilon > 0$ (here we used $L = o(\log p/\log\log p)$. Substituting the above back into (6.3) and simplifying, we find that

$$\sum_{a=0}^{m-1} \left(\Phi_{\mathcal{C},\Omega}(m,a) - \frac{1}{m}\right)^2 \le \frac{4m^4 N|\mathcal{I}|}{p^2} + O(m^4/p^{\frac{1}{2}-\varepsilon}) \le \frac{4m^4}{L(p)} + O(m^4/p^{\frac{1}{2}-\varepsilon}).$$

□

7. An application on the distribution of ℓ-th power residues and nonresidues

As an application of our results, we show how they can lead to uniform distribution results of ℓ-th power residues and nonresidues. First we consider $\ell = 2$. Let $\mathcal{C}$ to be the curve defined by $y^2 = x$, and let $L(p)$ be a function that tends to infinity with p, but of order $o(\log p/\log\log p)$, and let I be an integer such that $p - L(p) > I > L(p)$. The conditions in Theorem 3 are satisfied if we take $\mathcal{J} = (\alpha p, \beta p] \subseteq [0, (p-1)/2]$ and $\mathcal{I} \gg p^{1/2+\delta}$. In our application, we take $\mathcal{J} = (0, \beta p]$ ($\beta \le 1/2$), $\mathcal{I} = [0, p-1-I]$ (so that we avoid going back to $x = 0$).

We say $x \in \mathbb{F}_p^*$ is a *β-quadratic residue* if $x \equiv y^2 \pmod p$ for $y \in (0, \beta p]$, and x is a β-quadratic nonresidue if it is not a β-quadratic residue. Recall that $\Omega = \mathcal{I} \times \mathcal{J}$. In this setting, a point (x, y) on $\mathcal{C} \cap \Omega$ corresponds to the β-quadratic residue x modulo p (note that we manually excluded $x = 0$ in our interval $\mathcal{I}$). Therefore, the number of points on $\mathcal{C} \cap \Omega$ with $x \in \mathcal{I}$ equals the number of β-quadratic residues in $\mathcal{I}$. Applying Corollary 3 we see that for any positive integer m, the number of β-quadratic residues in $[x_0, x_0 + I)$ for $x_0 \in \mathcal{I}$ is uniformly distributed modulo m. Since inside an interval of length I, the number of β-residues and nonresidues always sum to I, we obtain uniform distribution for the β-nonresidues as well. More precisely, let $R_\beta(x_0, I)$ and $N_\beta(x_0, I)$ be the number of β-residues and nonresidues in the interval $[x_0, x_0 + I)$ respectively, and let

$$\Phi_{R,\beta,I}(m, a) = \frac{1}{p}\#\{x_0 \in [0, p - 1 - I] : R_\beta(x_0, I) \equiv a \pmod m\},$$
$$\Phi_{N,\beta,I}(m, a) = \frac{1}{p}\#\{x_0 \in [0, p - 1 - I] : N_\beta(x_0, I) \equiv a \pmod m\}.$$

Then we have the following.

Corollary 5. *If $m = o(L(p))^{1/6})$, then*

$$\Phi_{R,\beta,I}(m, a) = \frac{1}{m} + O\left(\frac{m^2}{\sqrt{L(p)}}\right),$$

uniformly for all $0 \le a \le m - 1$. The same holds with $\Phi_{R,\beta,I}(m, a)$ being replaced by $\Phi_{N,\beta,I}(m, a)$.

Note that if we take $\beta = 1/2$, we see that the quadratic residues and nonresidues are uniformly distributed among congruence classes modulo m.

If $L(p)$ is a function that tends to infinity with p, we fix an interval of length $I = L(p)$, and take $m = [L(p)^{1/7}]$. For any $x_0 \in [0, p - 1 - I]$, there are no β-quadratic residues (resp. nonresidues) inside the interval $[x_0, x_0 + I)$ only if $N_\beta(x_0, I) \equiv 0 \pmod m$ (resp. $N_\beta(x_0, I) \equiv I \pmod m$). By Corollary 5, there are at most

$$p\Phi_{R,\beta,I}(m, a) = \frac{p}{L(p)^{1/7}} + O\left(\frac{pL(p)^{2/7}}{\sqrt{L(p)}}\right) = \frac{p}{L(p)^{1/7}} + O\left(\frac{p}{L(p)^{3/14}}\right)$$

such values of x_0. We thus obtain the following result.

Corollary 6. *Let $L(p)$ be an integer function of p that tends to infinity with p. For all $x_0 \in [0, p - 1]$ except possibly $O(p/L(p)^{1/7})$ of them, there is a β-quadratic residue and a β-nonresidue inside the interval $[x_0, x_0 + L(p))$.*

Taking $\beta = 1/2$ gives Corollary 4 for the case $\ell = 2$.

For $\ell > 2$, there is no convenience choice of $\mathcal{I}$, $\mathcal{J}$ such that condition $(*)$ is satisfied, so we use Corollary 1 instead. Consider the curve $y^\ell = x$, and argue as the case $\ell = 2$, we see that $N_{\mathcal{C}}(x_0, I)$ equals ℓ times the number of ℓ-th power residue in the interval $[x_0, x_0 + I)$. Let μ be an ℓ-th root of unity and let $R_{\ell,\mu}(x_0, I)$ be the number of $x \in [x_0, x_0 + I)$ with $\frac{x}{p}_\ell = \mu$. Define

$$\Phi_{\ell,\mu,I}(m, a) = \frac{1}{p}\#\{x_0 \in [0, p - 1] : R_{\ell,\mu}(x_0, I) \equiv a \pmod m\}.$$

Invoking Corollary 1, for $GCD(\ell, m) = 1$ and $m = o(L(p)^{1/5})$, we have

$$\Phi_{\ell,1,I}(m,a) = \frac{1}{m} + O\left(\sqrt{\frac{m^3\ell^2}{L(p)}}\right). \tag{7.1}$$

For other $\mu \neq 1$, we let $\overline{\mu}$ be its inverse modulo p and consider the curve $y^2 = \overline{\mu}x$ to get a similar equation as (7.1) that is true with μ in place of 1 in the subindex. We sum them up in the following proposition.

Proposition 7.1. *If $GCD(m, \ell) = 1$ and $m = o(L(p))^{1/5})$, then*

$$\Phi_{\ell,\mu,I}(m,a) = \frac{1}{m} + O\left(\sqrt{\frac{m^3\ell^2}{L(p)}}\right),$$

uniformly for all $0 \leq a \leq m-1$ and all ℓ-th root of unity μ.

If $L(p)$ is a function that tends to infinity with p, we again fix an interval of length $I = L(p)$, and take $m = [L(p)^{1/7}]$ (if this m is not relatively prime to ℓ, add a small constant to it so that the new m is relatively prime to ℓ). A similar argument as in the case $\ell = 2$ then gives Corollary 4 for the case $\ell > 2$.

References

[1] M. V. Berry and M. Tabor, *Level clustering in the regular spectrum*, Proc. Royal Soc. London A **356** (1977), 375–394.

[2] J. Bourgain, T. Cochrane, J. Paulhus, and C. Pinner, *On the parity of k-th powers modulo p. A generalization of a problem of Lehmer*, Acta Arith. **147** (2011), no. 2, 173–203.

[3] A. Bucur, C. David, B. Feigon, and M. Lalín, *Fluctuations in the number of points on smooth plane curves over finite fields*, J. Number Theory **130** (2010), no. 11, 2528–2541.

[4] ———, *Statistics for traces of cyclic trigonal curves over finite fields*, Int. Math. Res. Not. IMRN (2010), no. 5, 932–967.

[5] T. H. Chan and I. Shparlinski, *Visible points on modular exponential curves*, Bull. Pol. Acad. Sci. Math. **58** (2010), no. 1, 17–22.

[6] S. Chatterjee and K. Soundararajan, *The distribution of short character sums*, To appear in IMRN.

[7] C. Cobeli and A. Zaharescu, *Generalization of a problem of Lehmer*, Manuscripta Math. **104** (2001), no. 3, 301–307.

[8] H. Davenport and P. Erdös, *The distribution of quadratic and higher residues*, Publ. Math. Debrecen **2** (1952), 252–265.

[9] W. Duke, J. B. Friedlander, and H. Iwaniec, *Equidistribution of roots of a quadratic congruence to prime moduli*, Ann. of Math. (2) **141** (1995), no. 2, 423–441.

[10] B. Dwork, *On The Zeta function of a hypersurface, II*, Ann. of Math. **80** (1964), no. 2, 227–299.

[11] M. Fujiwara, *Distribution of rational points on varieties over finite fields*, Mathematika **35** (1988), no. 2, 155–171.

[12] M. Hildebrand, *A survey of results on random random walks on finite groups*, Probab. Surv. **2** (2005), 33–63 (electronic).

[13] P. Kurlberg and Z. Rudnick, *The fluctuations in the number of points on a hyperelliptic curve over a finite field*, J. Number Theory **129** (2009), no. 3, 580–587.

[14] Y. Lamzouri, *The distribution of short character sums*, `arXiv:1106.6072 [math.NT]`.

[15] Y. Lamzouri and A. Zaharescu, *Randomness of character sums modulo m*, `arXiv:1104:4957 [MATH:NT]`.

[16] K.-H. Mak and A. Zaharescu, *Poisson type phenomena for points on hyperelliptic curves modulo p*, to appear in Funct. Approx. Comment. Math.

[17] G. Myerson, *The distribution of rational points on varieties defined over a finite field*, Mathematika **28** (1981), no. 2, 153–159 (1982).

[18] W. Narkiewicz, *Uniform distribution of sequences of integers in residue classes*, Lecture Notes in Mathematics, vol. 1087, Springer-Verlag, Berlin, 1984.

[19] Z. Rudnick and P. Sarnak, *The pair correlation function of fractional parts of polynomials*, Comm. Math. Phys. **194** (1998), no. 1, 61–70.
[20] Z. Rudnick, P. Sarnak, and A. Zaharescu, *The distribution of spacings between the fractional parts of $n^2\alpha$*, Invent. Math. **145** (2001), no. 1, 37–57.
[21] P. Sarnak, *Quantum chaos, symmetry and zeta functions. Lecture I. Quantum chaos*, Current developments in mathematics, 1997 (Cambridge, MA), Int. Press, Boston, MA, 1999, pp. 127–144.
[22] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, Séminaire Delange-Pisot-Poitou, 16e année (1974/75), Théorie des nombres, Fasc. 1, Exp. No. 20, Secrétariat Mathématique, Paris, 1975, p. 28.
[23] I. Shparlinski, *Primitive points on modular hyperbola*, Bull. Pol. Acad. Sci. Math. **54** (2006), no. 3-4, 193–200.
[24] I. Shparlinski and J. F. Voloch, *Visible points on curves over finite fields*, Bull. Pol. Acad. Sci. Math. **55** (2007), no. 3, 193–199.
[25] I. Shparlinski and A. Winterhof, *Visible points on multidimensional modular hyperbolas*, J. Number Theory **128** (2008), no. 9, 2695–2703.
[26] F. Spitzer, *Principles of random walks*, second ed., Springer-Verlag, New York, 1976, Graduate Texts in Mathematics, Vol. 34.
[27] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U. S. A. **34** (1948), 204–207.
[28] ———, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann et Cie., Paris, 1948.
[29] M. Xiong, *The fluctuations in the number of points on a family of curves over a finite field*, J. Théor. Nombres Bordeaux **22** (2010), no. 3, 755–769.
[30] A. Zaharescu, *Correlation of fractional parts of $n^2\alpha$*, Forum Math. **15** (2003), no. 1, 1–21.
[31] W. Zhang, *On a problem of D. H. Lehmer and its generalization*, Compositio Math. **86** (1993), no. 3, 307–316.
[32] ———, *A problem of D. H. Lehmer and its generalization. II*, Compositio Math. **91** (1994), no. 1, 47–56.

Department of Mathematics, University of Illinois at Urbana-Champaign, 273 Altgeld Hall, MC-382, 1409 W. Green Street, Urbana, Illinois 61801, USA
E-mail address: mak4@illinois.edu

Department of Mathematics, University of Illinois at Urbana-Champaign, 273 Altgeld Hall, MC-382, 1409 W. Green Street, Urbana, Illinois 61801, USA
E-mail address: zaharesc@math.uiuc.edu